

Sum Complexes and Uncertainty Numbers

Roy Meshulam *

December 17, 2012

Abstract

Let p be a prime and let $A \subset \mathbb{F}_p$. For $k < p$ let $X_{A,k}$ be the $(k-1)$ -dimensional complex on the vertex set \mathbb{F}_p with a full $(k-2)$ -skeleton whose $(k-1)$ -faces are $\sigma \subset \mathbb{F}_p$ such that $|\sigma| = k$ and $\sum_{x \in \sigma} x \in A$. The homology groups of $X_{A,k}$ with field coefficients are determined. In particular it is shown that if $|A| \leq k$ then $H_{k-1}(X_{A,k}; \mathbb{F}_p) = 0$. This implies a homological characterization of uncertainty numbers of subsets of \mathbb{F}_p : Let \mathbb{F} be algebraically closed, then $H_{k-1}(X_{A,k}; \mathbb{F}) \neq 0$ iff there exists an $0 \neq f \in \mathbb{F}[\mathbb{F}_p]$ with $\text{supp}(f) \subset A$ such that the endomorphism of $\mathbb{F}[\mathbb{F}_p]$ given by $g \rightarrow fg$ has rank at most $p-k$.

1 Introduction

Let p be a prime and let $\mathbb{F}_p = \{0, \dots, p-1\}$ be the field of order p . Denote by Δ_{p-1} the $(p-1)$ -simplex on the vertex set \mathbb{F}_p and let $\Delta_{p-1}^{(k)}$ be the k -dimensional skeleton of Δ_{p-1} . Let $A = \{a_1, \dots, a_m\}$ be a subset of \mathbb{F}_p and let $1 < k < p$. The *Sum Complex* $X_{A,k}$ was defined in [5] by

$$X_{A,k} = \Delta_{p-1}^{(k-2)} \cup \{\sigma \subset \mathbb{F}_p : |\sigma| = k, \sum_{x \in \sigma} x \in A\}.$$

$X_{A,k}$ is a $(k-1)$ -dimensional complex whose f -vector satisfies $f_i(X_{A,k}) = \binom{p}{i+1}$ for $0 \leq i \leq k-2$ and $f_{k-1}(X_{A,k}) = \frac{m}{p} \binom{p}{k} = \frac{m}{k} \binom{p-1}{k-1}$.

*Department of Mathematics, Technion, Haifa 32000, Israel. e-mail: meshulam@math.technion.ac.il .

Example: Let $p = 7$ and $A = \{0, 1, 3\} \subset \mathbb{F}_7$. Then $X_{A,3}$ is homotopy equivalent to the real projective plane \mathbb{RP}^2 , see Figure 1 in [5].

In this paper we study the homology of $X_{A,k}$ with field coefficients. Let \mathbb{F} be a field of characteristic ℓ . First suppose that $\ell \nmid p$ and let ω be a primitive p -th root of unity in the algebraic closure $\overline{\mathbb{F}}$. For $\beta = (b_1, \dots, b_k) \in \mathbb{F}_p^k$ let M_β be the $k \times m$ matrix given by $M_\beta(i, j) = \omega^{b_i a_j}$. Let

$$\mathcal{B}_k = \{(b_1, \dots, b_k) : 0 \leq b_1 < \dots < b_k \leq p-1\}.$$

The case $m = k$ of the following result is implicit in [5].

Theorem 1.1. *If $\text{char } \mathbb{F} \nmid p$ then*

$$\dim H_{k-1}(X_{A,k}; \mathbb{F}) = \frac{m}{k} \binom{p-1}{k-1} - \frac{1}{p} \sum_{\beta \in \mathcal{B}_k} \text{rank } M_\beta.$$

Our main result concerns the homology of $X_{A,k}$ with \mathbb{F}_p coefficients.

Theorem 1.2.

$$\dim H_{k-1}(X_{A,k}; \mathbb{F}_p) = \begin{cases} 0 & m \leq k \\ \left(\frac{m}{k} - 1\right) \binom{p-1}{k-1} & m > k. \end{cases} \quad (1)$$

Remarks:

- 1) The argument given in [5] for the case $m = k$ of Theorem 1.1 does not seem to extend to the modular case. The approach here is different and is also used in the proof of our main result Theorem 1.2.
- 2) The reduced Euler characteristic of $X_{A,k}$ is

$$\begin{aligned} \tilde{\chi}(X_{A,k}) &= -1 + \sum_{i=0}^{k-2} (-1)^i \binom{p}{i+1} + (-1)^{k-1} \frac{m}{p} \binom{p}{k} \\ &= (-1)^{k-1} \left(\frac{m}{k} - 1\right) \binom{p-1}{k-1}. \end{aligned} \quad (2)$$

Since $\tilde{H}_i(X_{A,k}; \mathbb{F}_p) = 0$ for $0 \leq i < k-2$ it follows that

$$\begin{aligned} \dim \tilde{H}_{k-2}(X_{A,k}; \mathbb{F}_p) &= \dim H_{k-1}(X_{A,k}; \mathbb{F}_p) - \left(\frac{m}{k} - 1\right) \binom{p-1}{k-1} \\ &= \begin{cases} \left(1 - \frac{m}{k}\right) \binom{p-1}{k-1} & m \leq k \\ 0 & m > k \end{cases} \end{aligned} \quad (3)$$

3) A classical result of Chebotarëv (see e.g. [7]) asserts that for $\mathbb{F} = \mathbb{Q}$ all M_β 's have full rank. Theorem 1.1 therefore implies that (1) and (3) remain true for $\tilde{H}_*(X_{A,k}; \mathbb{Q})$.

We next discuss an application of Theorems 1.1 and 1.2 to discrete uncertainty principles. Let K be a finite abelian group and let $\mathbb{F}[K]$ be the group algebra of K over the field \mathbb{F} . For an element $f \in \mathbb{F}[K]$ let $T_f : \mathbb{F}[K] \rightarrow \mathbb{F}[K]$ be given by $T_f g = fg$. The *uncertainty number* of a subset $A \subset K$ is defined by

$$u_{\mathbb{F}}(A) = \min\{\text{rank } T_f : \emptyset \neq \text{supp}(f) \subset A\}.$$

The motivation for this definition and terminology is as follows. Let m be the exponent of K and suppose \mathbb{F} contains a primitive m -th root of unity. Let \hat{K} denote the group of \mathbb{F} -valued characters of K . Identifying $\mathbb{F}[K]$ with the space of \mathbb{F} -valued functions on K , the Fourier Transform of a function $f \in \mathbb{F}[K]$ is the function $\hat{f} \in \mathbb{F}[\hat{K}]$ given by $\hat{f}(\chi) = \sum_{x \in K} \chi(-x)f(x)$. It is well known that $\text{rank } T_f = |\text{supp}(\hat{f})|$. Thus in the semisimple case

$$u_{\mathbb{F}}(A) = \min\{|\text{supp}(\hat{f})| : \emptyset \neq \text{supp}(f) \subset A\}. \quad (4)$$

The classical discrete uncertainty principle (see e.g. [1]) asserts that $u_{\mathbb{F}}(A) \geq \frac{|K|}{|A|}$ for any \mathbb{F} and $\emptyset \neq A \subset K$. While this bound is sharp when A is a coset of K , it can often be improved for particular choices of K , A and \mathbb{F} . One such example is a result of Tao [8] asserting that if $A \subset \mathbb{F}_p$ then $u_{\mathbb{C}}(A) = p - |A| + 1$. See [6] for an extension to general abelian groups. Here we note a simple relation between the homology of sum complexes and uncertainty numbers of subsets of \mathbb{F}_p .

Theorem 1.3. *If \mathbb{F} is algebraically closed then for any $A \subset \mathbb{F}_p$*

$$u_{\mathbb{F}}(A) = p - \max\{k : H_{k-1}(X_{A,k}; \mathbb{F}) \neq 0\}.$$

Example: It is easy to see that $u_{\mathbb{F}}(A) \geq p - \max A$ for any $A \subset \mathbb{F}_p$ and any field \mathbb{F} . Taking $A = \{0, 1, 3\} \subset \mathbb{F}_7$ it follows that $u_{\overline{\mathbb{F}_2}}(A) \geq 4$. On the other hand, as noted earlier $X_{A,3}$ is homotopy equivalent to \mathbb{RP}^2 , hence $H_2(X_{A,3}; \mathbb{F}_2) \neq 0$. Theorem 1.3 then implies that $u_{\overline{\mathbb{F}_2}}(A) = 4$. It can be checked that in fact $u_{\mathbb{F}_2}(A) = 4$.

Let C_p be the multiplicative cyclic group of order p and let $G = C_p^k$. In Section 2 we identify $H_{k-1}(X_{A,k}; \mathbb{F})$ with a certain subspace $\mathcal{H}(A)$ of skew-symmetric elements of the group algebra $\mathbb{F}[G]$. This characterization is used in Section 3 to prove Theorem 1.1. The proof of Theorem 1.2 given in Section 4 is more involved and depends additionally on some properties of generalized Vandermonde determinants over the group algebra $\mathbb{F}_p[G]$. Theorem 1.3 is derived in Section 5 as a direct consequence of Theorems 1.1 and 1.2. We conclude in Section 6 with some comments and open problems.

2 A Characterization of Cycles

Let $\mathcal{F}(\mathbb{F}_p^k, \mathbb{F})$ denote the space of \mathbb{F} -valued functions on \mathbb{F}_p^k . A function $\phi \in \mathcal{F}(\mathbb{F}_p^k, \mathbb{F})$ is *skew-symmetric* if $\phi(\gamma_{\sigma^{-1}(1)}, \dots, \gamma_{\sigma^{-1}(k)}) = \text{sgn}(\sigma)\phi(\gamma_1, \dots, \gamma_k)$ for all $(\gamma_1, \dots, \gamma_k) \in \mathbb{F}_p^k$ and σ in the symmetric group S_k . If $\text{char } \mathbb{F} = 2$ then ϕ is additionally required to satisfy $\phi(\gamma_1, \dots, \gamma_k) = 0$ if $\gamma_i = \gamma_j$ for some $i \neq j$. Let $\mathcal{A}(\mathbb{F}_p^k, \mathbb{F})$ be the space of skew-symmetric functions in $\mathcal{F}(\mathbb{F}_p^k, \mathbb{F})$.

Fix a generating set $\{x_1, \dots, x_k\}$ of G and let $x = (x_1, \dots, x_k) \in G^k$. For $\gamma = (\gamma_1, \dots, \gamma_k) \in \mathbb{F}_p^k$ we abbreviate $x^\gamma = \prod_{j=1}^k x_j^{\gamma_j}$. Let $q : \mathcal{F}(\mathbb{F}_p^k, \mathbb{F}) \rightarrow \mathbb{F}[G]$ be the \mathbb{F} -linear isomorphism given by

$$q(\phi) = \sum_{\gamma \in \mathbb{F}_p^k} \phi(\gamma) x^\gamma.$$

An element $s \in \mathbb{F}[G]$ is *homogenous of degree $d \in \mathbb{F}_p$* if $s = q(\phi)$ where

$$\text{supp}(\phi) \subset W_d = \{\alpha = (\alpha_1, \dots, \alpha_k) \in \mathbb{F}_p^k : \sum_{i=1}^k \alpha_i = d\}.$$

Let $\mathbb{F}[G]_d$ denote the space of degree d elements of $\mathbb{F}[G]$ and let ρ_d be the projection from $\mathbb{F}[G]$ onto $\mathbb{F}[G]_d$. An element $s \in \mathbb{F}[G]$ is *skew-symmetric* if $s = q(\phi)$ for some $\phi \in \mathcal{A}(\mathbb{F}_p^k, \mathbb{F})$. Let \mathcal{S} be the space of skew-symmetric elements of $\mathbb{F}[G]$ and let $\mathcal{S}_d = \mathcal{S} \cap \mathbb{F}[G]_d$.

The space of \mathbb{F} -valued $(k-1)$ -chains of $X_{A,k}$ is

$$C_{k-1}(X_{A,k}; \mathbb{F}) = \{\phi \in \mathcal{A}(\mathbb{F}_p^k, \mathbb{F}) : \text{supp}(\phi) \subset \cup_{a \in A} W_a\}.$$

A $(k-1)$ -chain $\phi \in C_{k-1}(X_{A,k}; \mathbb{F})$ is a $(k-1)$ -cycle of $X_{A,k}$ if

$$\sum_{a \in A} \phi(\alpha_1, \dots, \alpha_{i-1}, a - \sum_{\{j: j \neq i\}} \alpha_j, \alpha_{i+1}, \dots, \alpha_k) = 0 \quad (5)$$

for all fixed $1 \leq i \leq k$ and $(\alpha_1, \dots, \hat{\alpha}_i, \dots, \alpha_k) \in \mathbb{F}_p^{k-1}$. Let

$$\mathcal{H}(A) = \{s \in \bigoplus_{a \in A} \mathcal{S}_a : \sum_{a \in A} x_i^{-a} \rho_a(s) = 0 \text{ for all } 1 \leq i \leq k\}.$$

The homology space $H_{k-1}(X_{A,k}; \mathbb{F}) = Z_{k-1}(X_{A,k}; \mathbb{F})$ is characterized by the following

Claim 2.1.

$$q(H_{k-1}(X_{A,k}; \mathbb{F})) = \mathcal{H}(A).$$

Proof: Let $\phi \in C_{k-1}(X_{A,k}; \mathbb{F})$ and fix an $1 \leq i \leq k$. Then

$$\begin{aligned} \sum_{a \in A} x_i^{-a} \rho_a(q(\phi)) &= \sum_{a \in A} x_i^{-a} \sum_{(\alpha_1, \dots, \alpha_k) \in W_a} \phi(\alpha_1, \dots, \alpha_k) \prod_{j=1}^k x_j^{\alpha_j} \\ &= \sum_{a \in A} x_i^{-a} \sum_{(\alpha_j : j \neq i) \in \mathbb{F}_p^{k-1}} \phi(\alpha_1, \dots, \alpha_{i-1}, a - \sum_{j \neq i} \alpha_j, \alpha_{i+1}, \dots, \alpha_k) \left(\prod_{j \neq i} x_j^{\alpha_j} \right) x_i^{a - \sum_{j \neq i} \alpha_j} \\ &= \sum_{(\alpha_j : j \neq i) \in \mathbb{F}_p^{k-1}} \left(\sum_{a \in A} \phi(\alpha_1, \dots, \alpha_{i-1}, a - \sum_{j \neq i} \alpha_j, \alpha_{i+1}, \dots, \alpha_k) \right) \prod_{j \neq i} (x_j x_i^{-1})^{\alpha_j} = 0. \end{aligned}$$

Therefore $\sum_{a \in A} x_i^{-a} \rho_a(q(\phi)) = 0$ iff for all $(\alpha_j : j \neq i) \in \mathbb{F}_p^{k-1}$

$$\sum_{a \in A} \phi(\alpha_1, \dots, \alpha_{i-1}, a - \sum_{j \neq i} \alpha_j, \alpha_{i+1}, \dots, \alpha_k) = 0.$$

Hence the Claim follows from (5). □

3 The Semisimple Case

In this section we prove Theorem 1.1. We may assume that \mathbb{F} is algebraically closed. Let

$$\mathcal{R} = \{(r_a)_{a \in A} \in \mathcal{S}^A : \sum_{a \in A} x_i^{-a} r_a = 0 \text{ for all } 1 \leq i \leq k\}.$$

Let $y = \prod_{j=1}^k x_j$ and let $P \subset G$ be the cyclic group generated by y .

Claim 3.1. *The mapping $B : \mathbb{F}[P] \otimes_{\mathbb{F}} \mathcal{H}(A) \rightarrow \mathcal{R}$ given by*

$$B(u \otimes s) = (u\rho_a(s))_{a \in A}$$

is an isomorphism.

Proof: We first show that B is injective. Let $w = \sum_{j=0}^{p-1} y^j \otimes s_j \in \ker B$. Then $\sum_{j=0}^{p-1} y^j \rho_a(s_j) = 0$ for all $a \in A$. Since $y^j \rho_a(s_j) \in \mathcal{S}_{a+kj}$ it follows that $y^j \rho_a(s_j) = 0$ and hence $\rho_a(s_j) = 0$ for all $0 \leq j \leq p-1$ and $a \in A$. Therefore $w = 0$. To show surjectivity let $(r_a)_{a \in A} \in \mathcal{R}$. For $0 \leq i, j \leq p-1$ let

$$s_j = y^{-j} \sum_{a \in A} \rho_{a+kj}(r_a) \in \bigoplus_{a \in A} \mathcal{S}_a$$

and

$$t_{ij} = \sum_{a \in A} x_i^{-a} \rho_{a+kj}(r_a) \in \mathcal{S}_{kj}.$$

Then for any $0 \leq i \leq p-1$

$$0 = \sum_{a \in A} x_i^{-a} r_a = \sum_{a \in A} x_i^{-a} \sum_{j=0}^{p-1} \rho_{a+kj}(r_a) = \sum_{j=0}^{p-1} t_{ij}.$$

It follows that $t_{ij} = 0$ for all $0 \leq i, j \leq p-1$. Therefore

$$\sum_{a \in A} x_i^{-a} \rho_a(s_j) = \sum_{a \in A} x_i^{-a} y^{-j} \rho_{a+kj}(r_a) = y^{-j} t_{ij} = 0$$

and hence $s_j \in \mathcal{H}(A)$. Finally

$$\sum_{j=0}^{p-1} y^j \rho_a(s_j) = \sum_{j=0}^{p-1} y^j (y^{-j} \rho_{a+kj}(r_a)) = \sum_{j=0}^{p-1} \rho_{a+jk}(r_a) = r_a,$$

therefore $B(\sum_{j=0}^{p-1} y^j \otimes s_j) = (r_a)_{a \in A}$.

□

Claim 3.1 implies that $\dim \mathcal{R} = p \dim \mathcal{H}(A)$. Theorem 1.1 will thus follow from

Proposition 3.2.

$$\dim \mathcal{R} = m \binom{p}{k} - \sum_{\beta \in \mathcal{B}_k} \text{rank } M_\beta.$$

Proof: Recall that ω is a primitive p -th root of unity in $\mathbb{F} = \overline{\mathbb{F}}$. The Fourier Transform is the automorphism of $\mathcal{F}(\mathbb{F}_p^k, \mathbb{F})$ given by

$$\widehat{\phi}(\beta) = \sum_{\alpha \in \mathbb{F}_p^k} \phi(\alpha) \omega^{-\beta \alpha}.$$

Define an \mathbb{F} -linear isomorphism

$$\Phi : \mathcal{S}^A \rightarrow \bigoplus_{\beta \in \mathcal{B}_k} \mathbb{F}^m$$

as follows. For $r = (r_a)_{a \in A} \in \mathcal{S}^A$ where $r_a = q(\phi_a)$ and $\phi_a \in \mathcal{A}(\mathbb{F}_p^k, \mathbb{F})$ let

$$\Phi(r) = \left((\widehat{\phi_{a_j}}(\beta))_{j=1}^m : \beta \in \mathcal{B}_k \right).$$

Claim 3.3. Φ restricts to an isomorphism from \mathcal{R} onto $\bigoplus_{\beta \in \mathcal{B}_k} \ker M_\beta$.

Proof: For $1 \leq i \leq k$ let e_i be the i -th unit vector in \mathbb{F}_p^k . Then $\psi_i = q^{-1}(\sum_{a \in A} x_i^{-a} r_a) \in \mathcal{F}(\mathbb{F}_p^k, \mathbb{F})$ is given by

$$\psi_i(\alpha) = \sum_{a \in A} \phi_a(\alpha + a e_i).$$

For $\beta = (b_1, \dots, b_k) \in \mathbb{F}_p^k$

$$\begin{aligned} \widehat{\psi_i}(\beta) &= \sum_{\alpha \in \mathbb{F}_p^k} \sum_{a \in A} \phi_a(\alpha + a e_i) \omega^{-\beta \alpha} = \sum_{a \in A} \sum_{\alpha \in \mathbb{F}_p^k} \phi_a(\alpha) \omega^{-\beta(\alpha - a e_i)} \\ &= \sum_{a \in A} \omega^{b_i a} \sum_{\alpha \in \mathbb{F}_p^k} \phi_a(\alpha) \omega^{-\beta \alpha} = \sum_{a \in A} \omega^{b_i a} \widehat{\phi_a}(\beta). \end{aligned}$$

It follows that $r = (r_a)_{a \in A} \in \mathcal{R}$ iff $\psi_1 = \dots = \psi_k = 0$ iff

$$M_\beta \begin{bmatrix} \widehat{\phi_{a_1}}(\beta) \\ \vdots \\ \widehat{\phi_{a_m}}(\beta) \end{bmatrix} = \begin{bmatrix} \omega^{b_1 a_1} & \dots & \omega^{b_1 a_m} \\ \vdots & \ddots & \vdots \\ \omega^{b_k a_1} & \dots & \omega^{b_k a_m} \end{bmatrix} \begin{bmatrix} \widehat{\phi_{a_1}}(\beta) \\ \vdots \\ \widehat{\phi_{a_m}}(\beta) \end{bmatrix} = \begin{bmatrix} \widehat{\psi_1}(\beta) \\ \vdots \\ \widehat{\psi_m}(\beta) \end{bmatrix} = 0$$

for all $\beta = (b_1, \dots, b_k) \in \mathbb{F}_p^k$. Therefore $\Phi(\mathcal{R}) \subset \bigoplus_{\beta \in \mathcal{B}_k} \ker M_\beta$. The bijectivity of the restriction $\Phi|_{\mathcal{R}}$ follows from the bijectivity Φ .

□

By Claim 3.3

$$\begin{aligned} \dim \mathcal{R} &= \sum_{\beta \in \mathcal{B}_k} \dim \ker M_\beta = \sum_{\beta \in \mathcal{B}_k} (m - \operatorname{rank} M_\beta) \\ &= m \binom{p}{k} - \sum_{\beta \in \mathcal{B}_k} \operatorname{rank} M_\beta. \end{aligned}$$

□

4 The Modular Case

In subsections 4.1 and 4.2 we study certain properties of determinants of generalized Vandermonde matrices over the group algebra $\mathbb{F}_p[G]$. These results are then used in Section 4.3 to prove Theorem 1.2.

4.1 A Generalized Vandermonde

Recall that $\{x_1, \dots, x_k\}$ is a fixed generating set of G and $x = (x_1, \dots, x_k)$. For $\beta = (b_1, \dots, b_k) \in \mathcal{B}_k$ let

$$N_\beta = \begin{bmatrix} x_1^{-b_1} & \cdots & x_1^{-b_k} \\ \vdots & \ddots & \vdots \\ x_k^{-b_1} & \cdots & x_k^{-b_k} \end{bmatrix}.$$

Proposition 4.1.

$$\det N_\beta = w_\beta \prod_{1 \leq i < j \leq k} (x_i - x_j) \tag{6}$$

where w_β is a unit of $\mathbb{F}_p[G]$.

Recall the definition of Schur polynomials (see e.g. [2]). Let $\xi = (\xi_1, \dots, \xi_k)$ be a vector of variables. For a partition $\lambda = (\lambda_1 \geq \dots \geq \lambda_k)$ let

$$D_\lambda(\xi) = D_\lambda(\xi_1, \dots, \xi_k) = \det([\xi_i^{\lambda_j + k - j}]_{i,j=1}^k) \in \mathbb{Z}[\xi_1, \dots, \xi_k].$$

Note that for the zero partition $0 = (0, \dots, 0)$

$$D_0(\xi) = \det \begin{bmatrix} \xi_1^{k-1} & \xi_1^{k-2} & \dots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ \xi_k^{k-1} & \xi_k^{k-2} & \dots & 1 \end{bmatrix} = \prod_{1 \leq i < j \leq k} (\xi_i - \xi_j).$$

The Schur polynomial associated with λ is

$$s_\lambda(\xi) = \frac{D_\lambda(\xi)}{D_0(\xi)} \in \mathbb{Z}[\xi_1, \dots, \xi_k].$$

The dimension formula (see e.g. Proposition 5.21.2 in [2]) asserts that

$$s_\lambda(1, \dots, 1) = \prod_{1 \leq i < j \leq k} \frac{\lambda_i - \lambda_j + j - i}{j - i}. \quad (7)$$

Proof of Proposition 4.1: Let

$$\lambda = (\lambda_1, \dots, \lambda_k) = (p - b_1 - k + 1, p - b_2 - k + 2, \dots, p - b_k).$$

Then

$$\begin{aligned} \det N_\beta &= D_\lambda(x) = s_\lambda(x) D_0(x) \\ &= s_\lambda(x) \prod_{1 \leq i < j \leq k} (x_i - x_j). \end{aligned}$$

By (7) the image of $s_\lambda(x) \in \mathbb{F}_p[G]$ under the augmentation map $\mathbb{F}_p[G] \rightarrow \mathbb{F}_p$ is

$$s_\lambda(1, \dots, 1) \pmod{p} = \prod_{1 \leq i < j \leq k} \frac{b_j - b_i}{j - i} \pmod{p} \neq 0 \pmod{p}.$$

It follows that $w_\beta = s_\lambda(x)$ is invertible in $\mathbb{F}_p[G]$.

□

4.2 Skew-Symmetric Annihilators of $D_0(x)$

In this subsection we show

Proposition 4.2. *Let $s \in \mathcal{S}$. If $D_0(x)s = 0$ then $s = 0$.*

The proof of Proposition 4.2 depends on Proposition 4.3 below. Let \mathbb{N} denote the nonnegative integers and for $a, b \in \mathbb{N}$ let $[a, b] = \{a, \dots, b\}$. Let

$$\mathbb{N}_k = \{(\alpha_1, \dots, \alpha_k) \in \mathbb{N}^k : \alpha_i \neq \alpha_j \text{ if } i \neq j\}.$$

For $\alpha = (\alpha_1, \dots, \alpha_k)$, $\beta = (\beta_1, \dots, \beta_k) \in \mathbb{N}_k$ write $\alpha \preceq \beta$ if $\{\alpha_1, \dots, \alpha_k\}$ precedes $\{\beta_1, \dots, \beta_k\}$ in the lexicographic order on subsets of \mathbb{N} , i.e. if

$$\sum_{i=1}^k 2^{-\alpha_i} \geq \sum_{i=1}^k 2^{-\beta_i}.$$

Fix an $\alpha = (\alpha_1, \dots, \alpha_k) \in \mathbb{N}_k$ such that $\alpha_1 < \dots < \alpha_k$ and let

$$L = \{1 \leq i \leq k-1 : \alpha_i + 1 < \alpha_{i+1}\}.$$

Write $L = \{\ell_1 < \dots < \ell_{t-1}\}$ and let $\ell_0 = 0$, $\ell_t = k$. For $1 \leq i \leq t$ let $A_i = [\ell_{i-1} + 1, \ell_i]$. Let

$$\mathcal{G}_1(\alpha) = \{(\gamma, \sigma) \in \mathbb{N}_k \times S_k : \gamma \preceq \alpha \text{ and } \gamma_j - \sigma(j) = \alpha_j - j \text{ for all } j\}.$$

We'll need the following characterization of $\mathcal{G}_1(\alpha)$. Let S_A denote the symmetric group on a set A . Let $T = S_{A_1} \times \dots \times S_{A_t}$ be the Young subgroup of S_k corresponding to the partition $[k] = \cup_{i=1}^t A_i$. Let

$$\mathcal{G}_2(\alpha) = \{(\gamma, \sigma) \in \mathbb{N}_k \times T : \gamma_j = \alpha_{\sigma(j)} \text{ for all } j\}.$$

Proposition 4.3. $\mathcal{G}_1(\alpha) = \mathcal{G}_2(\alpha)$

Proof: We first show that $\mathcal{G}_2(\alpha) \subset \mathcal{G}_1(\alpha)$. Let $(\gamma, \sigma) \in \mathcal{G}_2(\alpha)$ and let $1 \leq j \leq k$. If $j \in A_i$ then $\sigma(j) \in A_i$ and hence $\alpha_{\sigma(j)} - \alpha_j = \sigma(j) - j$. Therefore

$$\gamma_j - \sigma(j) = \alpha_{\sigma(j)} - \sigma(j) = \alpha_j - j$$

and so $(\gamma, \sigma) \in \mathcal{G}_1(\alpha)$. For the other direction let $(\gamma, \sigma) \in \mathcal{G}_1(\alpha)$. Write $\gamma = (\gamma_1, \dots, \gamma_k)$ and let $\pi \in S_k$ such that $\gamma_{\pi(1)} < \dots < \gamma_{\pi(k)}$.

Claim 4.4. For $1 \leq i \leq t$ and $j \in A_i$

- (a) $\sigma(\pi(j)) = j$.
- (b) $\gamma_{\pi(j)} = \alpha_j$.
- (c) $\pi(j) \in A_i$.

Proof: We argue by induction on j . Suppose (a),(b) and (c) hold for all $j' < j$. (a) implies that $\{\sigma(\pi(j')) : j' < j\} = [j-1]$ and hence $\sigma(\pi(j)) \geq j$. Therefore

$$\alpha_j - j \geq \alpha_j - \sigma(\pi(j)). \quad (8)$$

Next note that by (b) $\gamma_{\pi(j')} = \alpha_{j'}$ for all $j' < j$. As $\gamma \preceq \alpha$ it follows that $\alpha_j \geq \gamma_{\pi(j)}$ and therefore

$$\alpha_j - \sigma(\pi(j)) \geq \gamma_{\pi(j)} - \sigma(\pi(j)) = \alpha_{\pi(j)} - \pi(j). \quad (9)$$

Finally (c) implies that $\{\pi(j') : 1 \leq j' \leq \ell_{i-1}\} = [1, \ell_{i-1}]$ and therefore $\pi(j) \geq \ell_{i-1} + 1$. Together with the assumption $j \in A_i$ it follows that

$$\alpha_{\pi(j)} - \pi(j) \geq \alpha_{\ell_{i-1}+1} - (\ell_{i-1} + 1) = \alpha_j - j. \quad (10)$$

It follows that the three inequalities in (8),(9),(10) are in fact equalities. Therefore $\sigma(\pi(j)) = j$, $\gamma_{\pi(j)} = \alpha_j$ and $\alpha_{\pi(j)} = \alpha_j + (\pi(j) - j)$ respectively establishing (a),(b),(c) for j .

□

Claim 4.4 implies that $\sigma = \pi^{-1} \in T$ and that $\gamma_j = \alpha_{\sigma(j)}$ for all $1 \leq j \leq k$. Therefore $(\gamma, \sigma) \in \mathcal{G}_2(\alpha)$.

□

Proof of Proposition 4.2: Let $s \in \mathcal{S}$ such that $D_0(x)s = 0$ and write $s = q(\phi)$ with $\phi \in \mathcal{A}(\mathbb{F}_p^k, \mathbb{F}_p)$. We have to show that $\phi = 0$. By assumption

$$\begin{aligned} 0 = D_0(x)s &= \sum_{\sigma \in S_k} \text{sgn}(\sigma) \prod_{j=1}^k x_j^{k-\sigma(j)} \sum_{\gamma=(\gamma_1, \dots, \gamma_k) \in \mathbb{F}_p^k} \phi(\gamma) \prod_{j=1}^k x_j^{\gamma_j} \\ &= \sum_{\gamma=(\gamma_1, \dots, \gamma_k) \in \mathbb{F}_p^k} \sum_{\sigma \in S_k} \text{sgn}(\sigma) \phi(\gamma) \prod_{j=1}^k x_j^{\gamma_j + k - \sigma(j)}. \end{aligned} \quad (11)$$

Suppose for contradiction that $\phi \neq 0$ and let

$$\alpha = (\alpha_1, \dots, \alpha_k) = \max\{\gamma \in \mathcal{B}_k : \phi(\gamma) \neq 0\}$$

where the maximum is taken with respect to \preceq . Let $\lambda \in \mathbb{F}_p$ denote the coefficient of $\prod_{j=1}^k x_j^{\alpha_j+k-j}$ in the expansion of $D_0(x)s$ in the standard basis $\{x^\beta : \beta \in \mathbb{F}_p^k\}$. Note that if

$$\prod_{j=1}^k x_j^{\alpha_j+k-j} = \prod_{j=1}^k x_j^{\gamma_j+k-\sigma(j)}$$

then for all $1 \leq j \leq k$

$$\alpha_j - j = \gamma_j - \sigma(j) \pmod{p}.$$

Since

$$-1 \leq \alpha_j - j \leq p - 1 - k$$

and

$$-k \leq \gamma_j - \sigma(j) \leq p - 2$$

it follows that

$$\alpha_j - j = \gamma_j - \sigma(j).$$

Hence, Eq. (11) and Proposition 4.3 imply that

$$\begin{aligned} \lambda &= \sum_{(\gamma, \sigma) \in \mathcal{G}_1(\alpha)} \text{sgn}(\sigma) \phi(\gamma) = \sum_{(\gamma, \sigma) \in \mathcal{G}_2(\alpha)} \text{sgn}(\sigma) \phi(\gamma) \\ &= \sum_{\sigma \in S_{A_1} \times \cdots \times S_{A_t}} \text{sgn}(\sigma) \phi(\alpha_{\sigma(1)}, \dots, \alpha_{\sigma(k)}) \\ &= |S_{A_1} \times \cdots \times S_{A_t}| \phi(\alpha) = \prod_{i=1}^t (\ell_i - \ell_{i-1})! \phi(\alpha). \end{aligned}$$

Since $\ell_t = k < p$ it follows that $\prod_{i=1}^t (\ell_i - \ell_{i-1})! \not\equiv 0 \pmod{p}$ and so $\lambda \neq 0$. Therefore $D_0(x)s \neq 0$, a contradiction.

□

4.3 Homology of $X_{A,k}$ over \mathbb{F}_p

In this subsection we prove Theorem 1.2. We first consider the case $m = k$.

Theorem 4.5. *If $|A| = k$ then $H_{k-1}(X_{A,k}; \mathbb{F}_p) = 0$.*

Proof: Let $A = \{a_1, \dots, a_k\}$ where $\alpha = (a_1, \dots, a_k) \in \mathcal{B}_k$. Let $\phi \in H_{k-1}(X_{A,k}; \mathbb{F}_p)$ and let $s = q(\phi)$. By Claim 2.1

$$N_\alpha \begin{bmatrix} \rho_{a_1}(s) \\ \vdots \\ \rho_{a_k}(s) \end{bmatrix} = \begin{bmatrix} x_1^{-a_1} & \cdots & x_1^{-a_k} \\ \vdots & \ddots & \vdots \\ x_k^{-a_1} & \cdots & x_k^{-a_k} \end{bmatrix} \begin{bmatrix} \rho_{a_1}(s) \\ \vdots \\ \rho_{a_k}(s) \end{bmatrix} = 0.$$

Therefore $\det N_\alpha \cdot \rho_a(s) = 0$ for all $a \in A$. Proposition 4.1 implies that $D_0(x)\rho_a(s) = 0$ and hence $\rho_a(s) = 0$ by Proposition 4.2. It follows that $\phi = 0$ and so $H_{k-1}(X_{A,k}; \mathbb{F}_p) = 0$.

□

Proof of Theorem 1.2: Let $|A| = m \geq k$ and let A' be an arbitrary subset of A of cardinality k . Theorem 1.2 and Eq. (2) imply that $\tilde{H}_*(X_{A',k}; \mathbb{F}_p) = 0$. Hence by the exact sequence

$$\begin{aligned} 0 &= H_{k-1}(X_{A',k}; \mathbb{F}_p) \rightarrow H_{k-1}(X_{A,k}; \mathbb{F}_p) \rightarrow \\ &\rightarrow H_{k-1}(X_{A,k}, X_{A',k}; \mathbb{F}_p) \rightarrow \tilde{H}_{k-2}(X_{A',k}; \mathbb{F}_p) = 0 \end{aligned}$$

it follows that

$$\begin{aligned} \dim H_{k-1}(X_{A,k}; \mathbb{F}_p) &= \dim H_{k-1}(X_{A,k}, X_{A',k}; \mathbb{F}_p) \\ &= f_{k-1}(X_{A,k}) - f_{k-1}(X_{A',k}) = \left(\frac{m}{k} - 1\right) \binom{p-1}{k-1}. \end{aligned}$$

□

5 Uncertainty Numbers and Homology

Proof of Theorem 1.3: Let $\text{char } \mathbb{F} = \ell$ and consider two cases:

(i) $\ell \nmid p$. For $\lambda = (\lambda_1, \dots, \lambda_m) \in \mathbb{F}^m$ let $f_\lambda : \mathbb{F}_p \rightarrow \mathbb{F}$ be given by $f_\lambda = \sum_{j=1}^m \lambda_j \delta_{a_j}$. Then $\text{supp}(f) \subset A$ and for $\beta = (b_1, \dots, b_k) \in \mathbb{F}_p^k$

$$M_\beta \lambda = \left(\sum_{j=1}^m \lambda_j \omega^{b_i a_j} \right)_{i=1}^k = \left(\hat{f}_\lambda(-b_i) \right)_{i=1}^k. \quad (12)$$

Theorem 1.1 implies that $H_{k-1}(X_{A,k}; \mathbb{F}) \neq 0$ iff $\text{rank } M_\beta < m$ for some $\beta = (b_1, \dots, b_k) \in \mathcal{B}_k$. On the other hand, (12) implies that $\text{rank } M_\beta < m$ iff there exists a $0 \neq \lambda \in \mathbb{F}^m$ such $\widehat{f}_\lambda(-b_i) = 0$ for $1 \leq i \leq k$. It follows that $H_{k-1}(X_{A,k}; \mathbb{F}) \neq 0$ iff there exists a nonzero $f : \mathbb{F}_p \rightarrow \mathbb{F}$ such that $\text{supp}(f) \subset A$ and $|\text{supp}(\widehat{f})| \leq p - k$.

(ii) $\ell = p$. Let \mathbb{F} be a field of characteristic p . By Theorem 1.2

$$p - \max\{k : H_{k-1}(X_{A,k}; \mathbb{F}) \neq 0\} = p - m + 1.$$

It thus suffices to show that $u_{\mathbb{F}}(A) = p - m + 1$. Let $f : \mathbb{F}_p \rightarrow \mathbb{F}$ be a function with $\emptyset \neq \text{supp}(f) \subset A = \{a_1, \dots, a_m\}$ and let $g(x) = \sum_{i=1}^m f(a_i)x^{a_i} \in \mathbb{F}[x]$. Then

$$\begin{aligned} \text{rank } T_f &= p - \deg \gcd(g(x), x^p - 1) \\ &= p - \deg \gcd(g(x), (x - 1)^p) = p - \mu(g) \end{aligned} \tag{13}$$

where $\mu(g)$ is the multiplicity of 1 as a root of $g(x)$. By a result of Frenkel (Lemma 2 in [3]), $\mu(g) \leq m - 1$ and hence $u_{\mathbb{F}}(A) \geq p - m + 1$. For the other direction note that the space of polynomials

$$\mathcal{P} = \{g(x) \in \mathbb{F}[x] : \deg g \leq p - 1, \mu(g) \geq m - 1\}$$

satisfies $\dim_{\mathbb{F}} \mathcal{P} = p - m + 1$. Hence \mathcal{P} contains a nonzero g of the form $g(x) = \sum_{i=1}^m \lambda_i x^{a_i}$. It follows by (13) that $0 \neq f = \sum_{i=1}^m \lambda_i \delta_{a_i} : \mathbb{F}_p \rightarrow \mathbb{F}$ satisfies $\text{rank } T_f \leq p - m + 1$. Therefore $u_{\mathbb{F}}(A) \leq p - m + 1$.

□

6 Concluding Remarks

We mention two problems related to the results of this paper.

- Let X be a $(k-1)$ -dimensional complex X with $N = f_{k-1}(X)$ facets. It was observed by G. Kalai, S. Weinberger and the author that the torsion subgroup $H_{k-2}(X)_{\text{tor}}$ satisfies $|H_{k-2}(X)_{\text{tor}}| \leq \sqrt{k}^N$. Kalai on the other hand showed [4] that there exist X 's with $|\tilde{H}_{k-2}(X)_{\text{tor}}| \geq \sqrt{k/e}^N$. Computer experiments indicate that the \mathbb{Q} -acyclic sum complexes obtained by taking $|A| = k$ often have large torsion. For example, $A =$

$\{0, 1, 19\} \subset \mathbb{F}_{83}$ satisfies $|H_1(X_{A,3})| > 1.17^N$ where $N = f_2(X_{A,3}) = \binom{82}{2}$. Note that the base of the exponent 1.17 is slightly bigger than the constant $\sqrt{3/e} \doteq 1.05$ in Kalai's lower bound. It view of this it would be interesting to determine (or estimate) the maximum torsion of sum complexes.

- Theorem 1.3 characterizes the uncertainty number $u_{\mathbb{F}}(A)$ with $A \subset K = \mathbb{F}_p$ and \mathbb{F} algebraically closed, in terms of the homology of $X_{A,k}$ over \mathbb{F} . It would be useful to find appropriate extensions of this characterization to general finite groups K and arbitrary fields \mathbb{F} .

ACKNOWLEDGMENTS

Research supported by a grant from the Israel Science Foundation with additional partial support from ERC Advanced Research Grant no 267165 (DISCONV) and ESF grant (ACAT).

The author would like to thank Shmuel Weinberger for helpful discussions.

References

- [1] D.L. Donoho and P.B. Stark, Uncertainty principles and signal recovery, *SIAM J. Applied Math.* **49**(1989) 906-931.
- [2] P. Etingof, Introduction to Representation Theory, Student Mathematical Library Vol. 59, AMS, 2011.
- [3] P. E. Frenkel, Simple proof of Chebotarev's theorem on roots of unity, arXiv:math/0312398.
- [4] G. Kalai, Enumeration of \mathbb{Q} -acyclic simplicial complexes, *Israel J. Math.* **45**(1983) 337-351.
- [5] N. Linial, R. Meshulam and M. Rosenthal, Sum complexes - a new family of hypertrees, *Discrete Comput. Geom.*, **44**(2010) 622-636.
- [6] R. Meshulam, An uncertainty inequality for finite abelian groups, *European J. of Combinatorics*, **27**(2006) 63-67.

- [7] P. Stevenhagen and H. W. Lenstra, Chebotarëv and his density theorem, *Math. Intelligencer* **18**(1996) 26–37.
- [8] T. Tao, An uncertainty principle for cyclic groups of prime order, *Math. Res. Lett.* **12**(2005)121-127.